

Amendments to the Claims

1. (Currently Amended) A computer-readable medium having computer-executable instructions for operating a policy agent of a network for performing steps comprising:
 - detecting a network connection from a client computer on the network;
 - composing a challenge for authenticating a user of the client computer associated with said network connection, the challenge being encrypted with a private key of the policy agent;
 - transmitting the challenge to the client computer;
 - receiving a response from the client computer;
 - decrypting the response using a public key of the user to obtain a first message digest value;
 - receiving network data through the network connection with the client computer;
 - calculating a second message digest value based on the challenge and the received network data;
 - comparing the first and second message digest values to determine whether a match is found; and
 - ~~deciding whether to accept the received network data, the deciding based, at least in part, on a result of the comparing step~~
if a match is found, then forwarding the network data to their specified recipient, else not forwarding the network data to their specified recipient.
2. (Original) A computer-readable medium as in claim 1, wherein the policy agent is a firewall.
3. (Previously Presented) A computer-readable medium as in claim 1, wherein the step of composing includes encrypting the challenge with a public key of the user.
4. (Original) A computer-readable medium as in claim 3, wherein the step of decrypting includes decrypting the response with a private key of the policy agent.
5. (Original) A computer-readable medium as in claim 1, wherein the step of composing includes generating a third digest value from data including a time value, and encrypting the third digest value with the private key of the policy agent.

In re Application of: Gunter et al.
Application No.: 09/436,135

6. (Original) A computer-readable medium as in claim 1, wherein the received network data are in a form of packets, and the step of calculating calculates the second message digest value based on a pre-selected number of packets of the received network data.
7. (Original) A computer-readable medium as in claim 1, having further computer-executable instructions for performing network access policies on the received network data according to the identity of the user after a match between the first and second message digest values is found.

8. (Currently Amended) A method of authenticating a user using a client computer on a network to transmit network data through a policy agent of the network, comprising the steps of:

detecting by the policy agent a network connection from the client computer for transmitting network data of the user;

receiving by the policy agent network data transmitted through the network connection from the client computer;

obtaining, by the policy agent, an identity of the user and a public key of the user;

composing, by the policy agent, a challenge encrypted with a private key of the policy agent;

sending the challenge to the client computer;

decrypting, by the client computer, the challenge;

generating, by the client computer, a first message digest value based on the challenge and the network data of the user;

encrypting, by the client computer, the first message digest value with a private key of the user to create a response;

sending the response to the policy agent;

decrypting, by the policy agent, the response to obtain the first message digest value;

calculating, by the policy agent, a second message digest value based on the challenge and the network data received through the network connection from the client computer;

comparing the first and second message digest values to determine whether there is a match therebetween, and

~~deciding whether to accept the received network data, the deciding based, at least in part, on a result of the comparing step~~

if a match is found, then forwarding, by the policy agent, the network data to their specified recipient, else not forwarding the network data to their specified recipient.

9. (Original) A method as in claim 8, further including the step of applying network policies by the policy agent on the received network data based on the identity of the user after a match between the first and second message digest values is found.

In re Application of: Gunter et al.
Application No.: 09/436,135

10. (Original) A method as in claim 8, wherein the step of composing the challenge includes encrypting the challenge with the public key of the user.
11. (Original) A method as in claim 8, wherein the step of encrypting by the client computer includes encrypting the first message digest value with a public key of the policy agent.
12. (Previously Presented) A method as in claim 8, wherein the step of composing the challenge includes generating a third message digest value based on data including a time value and encrypting the third message digest value to form the challenge.
13. (Original) A method as in claim 8, wherein the received network data are in a form of packets, and the step of generating by the client computer generates the first message digest value based on data of a pre-selected number of packets of the received network data.
14. (Original) A method as in claim 8, wherein the step of generating by the client computer generates the first message digest value based on a random number, data decrypted from the challenge, and data of the pre-selected packets of the received network data.
15. (Original) A method as in claim 8, wherein the policy agent is a firewall of the network.